AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

FILED
MAR 07 2019
CARMELITA REEDER SHINN, CLERK
U.S. DIST. COURT, WESTERN DIST. OKLA.
BY RM ,DEPUTY

for the

Western District of Oklahoma

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

User Records maintained by Match LLC.

Case No. M-19-113-STE

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Apple Inc. user records maintained by the Custodian of Records, Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.;

located in the Western District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized)*:

records pertaining to iClound accounts associated with the email address: Gvg27ville@yahoo.com; telephone number 3015188543; including conversations, identifying information (names, email addresses, phone numbers, etc.), any available sent or unsent photos or videos; Messages; conversations; MMS; SMS.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Article 120c	Aggravated Sexual Contact

The application is based on these facts:
See Continuation Sheet.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Christopher D. Deeb, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: Mar 7, 2019

Judge's signature

City and state: OKC, OK

Shon T. Erwin, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Christopher D. Deeb, a Special Agent (SA) with the United States Army Criminal Investigation Division (CID), being duly sworn, depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the above-listed Apple ID that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cuptertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I have been employed as a Special Agent of the U.S. Army CID since August of 2014, and am currently assigned as a Special Agent to the Fort Sill CID Office. While employed by the U.S. Army, I have investigated federal criminal violations related to high technology or cybercrime, child pornography, rape, abusive sexual contact, and conspiracy. I have gained experience through training at the U.S. Army Military Police School (USAMPS) and everyday work relating to conducting these types of investigations. I have received specific training in the area of rape while I attended the Special Victims Capabilities Course (SVCC), Domestic Violence Investigation Training (DVIT), Child Abuse Prevention Investigative Techniques (CAPIT), and Advanced Crime Scenes Investigative Training (ACSIT) course with the U.S. Army, which focused on in depth investigative techniques and procedures. Moreover, I am a

federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, 2252A, and 2422(b), and I am authorized by the Attorney General to request a search warrant.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. This affidavit is submitted in support of an application for a search warrant for the contents of and information pertaining to the Apple iCloud account, Gvg27ville@yahoo.com ("subject account"), and phone number 3015188543 associated with that account, which are more specifically described in Attachment A, for contraband and evidence, fruits, and instrumentalities of violations of Article 120c (Aggravated Sexual Contact), UCMJ, and 120d (Abusive Sexual Contact), UCMJ; which items are more specifically described in Attachment B.

PROBABLE CAUSE

5. On 24 Oct 18, PVT M.T. was interviewed and provided a sworn statement to this office wherein she described how she was assaulted by PV2 King. PVT M.T. explained how she went to obtain ice for her Camel Pack and was escorted by PV2 King. PVT M.T. said, upon entering the room where she was alone with PV2 King, PV2 King grabbed her by the neck with his hand and began to squeeze. PVT M.T. said PV2 King used this hold to manipulate her face to kiss her. PVT M.T. stated PV2 King's grasp around her neck began to hinder her ability to draw a breath. PVT M.T. said PV2 King then began to attempt to remove her physical training (PT)

pants. PVT M.T. remembered thinking she was about to be raped. PVT M.T. stated she was able to escape the grasp of PV2 King and leave the room.

6. On 5 Nov 18, PV2 Demarco King provided a sworn statement to this office wherein he denied he assaulted PVT M.T. PV2 King maintained he was invited into the room by PVT M.T. for a consensual sexual encounter. PV2 King said PVT M.T. sent him a text message, which he no longer had on his cell phone, requesting he meet her in the room. PV2 King stated in the interview that the text message, which was sent to him by PVT M.T. on 22 Oct 18, was backed up to his iCloud account, but he was unable to retrieve it. PV2 King provided written consent to this office for the search of his iCloud account and provided his Apple ID and phone number.

7. On 5 Nov 18, SA Deeb completed a physical extraction of all the information on PV2 King's cell phone, which did not reveal the text message PV2 King spoke of. The extraction was completed using the Physical Analyzer on the Stand-Alone computer located within the CID office.

8. On 14 Nov 18, PV2 King was re-interviewed, wherein he admitted he lied about him never touching, or grabbing, PVT M.T. around the neck. PV2 King maintained he was lured into the room by PVT M.T. with the expectation of a consensual sexual encounter. PV2 King stated he grabbed PVT M.T. around her neck, not in an attempt to strangle her, but "more like in a sexual manner".

9. On 11 Dec 18, SA Deeb coordinated with the records department, Apple legal team, and informed them that this office had obtained written consent from PV2 King for

information contained within his iCloud account. A response was received which stated "the most appropriate approach is for a legal request to be obtained seeking the information from Apple."

INFORMATION REGARDING APPLE ID AND iCLOUD

10. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

11. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contact, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com or any Internet-connected device. For example, iCloud Mail enable a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. Furthermore, through the iCloud service, Apple offers call history syncing as a convenience to their customers so they can return calls from any of their devices. Apple stores these records in its iCloud service. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

12. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

13. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user access and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

14. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means

of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID' and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

15. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP address that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

16. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Medial Access Control address

("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

17. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and setting, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud.

18. On 5 Nov 18, PV2 King provided a statement wherein he described how he received a "text message" from the victim inviting him to a consensual sexual encounter. In my

training and experience, evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

19. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. It has also been my experience where the requested items were used to exclude the innocent from further suspicion.

20. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

21. Based on the statements made by PV2 King and PVT M.T., I believe Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

22. I anticipate executing this warrant under the Electronic Communication Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

23. Based on the forgoing, I request that the Court issue the proposed search warrant.

24. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States that has jurisdiction over the offense being investigated."

25. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

26. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

Christopher D. Deeb
Special Agent
U.S. Army Criminal Investigation Division

Subscribed to and sworn before me this 7 day of MARCH, 2019.

Shon T. Erwin

HONORABLE SHON T. ERWIN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Gvg27ville@yahoo.com and phone number 3015188543 (the "account") associated with that account that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cuptertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple., including any records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, and methods of connecting;

b. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

c. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, My Photo Stream, iCloud Photo Library, iCloud Drive, and all address books, contact and buddy lists, images, videos, voicemails, device setting, and bookmarks;

d. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone longs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers), all synced call detail records, containing any of the following; calls made and received, numbers dialed, date and time and duration, missed and forwarded calls, whether the calls were made through the phone interface or through the Apple CallKit via any third-party communications applications;

e. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

f. All records pertaining to the types of service used.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and/or instrumentalities of violations of Article 120c (Aggravated Sexual Contact), UCMJ, and 120d (Abusive Sexual Contact), UCMJ involving PV2 King since 22 Oct 18, including, for each account or identifier listed on Attachment A, information pertaining to communications, text messages, SMS, MMS between PV2 King and PVT M.T.

a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

c. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

d. Evidence that may identify any co-conspirators or aiders and abettors, including records that reveal their whereabouts.

The Provider shall deliver the information set forth above via United States mail, courier, or e-mail to:

SA Christopher Deeb
Fort Sill CID Office
2635 Miner Road
Fort Sill, OK 73503
Christopher.d.deeb.mil@mail.mil

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Apple Inc., and my official title is _____. I am a custodian of records for Apple Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Apple Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Apple Inc.; and

c. such records were made by Apple Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature